Electronic identification for universities: Building cross-border services based on the eIDAS infrastructure

information

MDPI

Article

Electronic Identification for Universities: Building Cross-Border Services Based on the eIDAS Infrastructure †

Diana Berbecaru *, Antonio Lioy and Cesare Cameroni

Politecnico di Torino, Dip. di Automatica e Informatica, Corso Duca degli Abruzzi 24, 10129 Torino, Italy; lioy@polito.it (A.L.); cesare.cameroni@polito.it (C.C.)

* Correspondence: diana.berbecaru@polito.it

† This paper is an extended version of the paper previously published by the authors in Proceedings of the 2018 22nd International Conference on System Theory, Control and Computing (ICSTCC 2018), Sinaia, Romania, 10–12 October 2018; pp. 691–696.

Received: 08 April 2019; Accepted: 30 May 2019; Published: 12 June 2019

Abstract: The European Union (EU) Regulation 910/2014 on electronic IDentification, Authentication, and trust Services (eIDAS) for electronic transactions in the internal market went into effect on 29 September 2018, meaning that EU Member States are required to recognize the electronic identities issued in the countries that have notified their eID schemes. Technically speaking, a unified interoperability platform—named eIDAS infrastructure—has been set up to connect the EU countries' national eID schemes to allow a person to authenticate in their home EU country when getting access to services provided by an eIDAS-enabled Service Provider (SP) in another EU country. The eIDAS infrastructure allows the transfer of authentication requests and responses back and forth between its nodes, transporting basic attributes about a person, e.g., name, surname, date of birth, and a so-called eIDAS identifier. However, to build new eIDAS-enabled services in specific domains, additional attributes are needed. We describe our approach to retrieve and transport new attributes through the eIDAS infrastructure, and we detail their exploitation in a selected set of academic services. First, we describe the definition and the support for the additional attributes in the eIDAS nodes. We then present a solution for their retrieval from our university. Finally, we detail the design, implementation, and installation of two eIDAS-enabled academic services at our university: the eRegistration in the Erasmus student exchange program and the Login facility with national eIDs on the university portal.

Keywords: electronic identity; eIDAS infrastructure; security; academic attributes; user authentication

1. Introduction

Today, the online environment and the availability of computing machines for millions of users worldwide allow for the exchange and processing of larger amounts of information than ever before, which can significantly speed-up the public administration (PA) processes or the execution of online financial transactions.

Typically, to access online public or private services (e.g., offered by universities, public offices, or private companies), citizens register directly with every Service Provider (SP). During the registration phase, SP stores several attributes associated to the citizen (e.g., name, surname, address, age), as well as their unique national identifier, like a fiscal code or social security number. In addition, SP also stores a set of credentials (e.g., username and password) that the citizen can later use for authentication purposes.

Some public or private companies issue smart cards to persons, containing identification data (e.g., photo or biometric data), possible user profile data (e.g., user ID inside the organization),

and cryptographic material (e.g., digital certificate and corresponding private key). These cards can be used for authentication and digital signing purposes. The smart card could be either a national ID card (issued by a governmental or PA office) containing various identification data (like a photo or biometric data) along with the cryptographic material, or it could be a card issued by an organization (like an university) which contains user profile data (like a user ID inside the organization and other personal data) and the digital certificate(s) to be used for authentication and digital signing purposes.

In this simple model, the 'producer' of the user profile—that is, the entity that associates identity data to a person together with that person's authentication credentials—is also its 'consumer', i.e., the SP itself implements the services requiring the authentication credentials registered in the first place. In general, smart cards issued by one provider are not automatically recognized by other SPs. Thus, today, users end up with having several usernames, passwords, and smart cards to access various SP services. Moreover, several solutions exist for authenticating citizens across countries: Some countries continue to use cards on a wide scale, other countries exploit both cards and usernames and passwords, while mobile solutions exploiting personal mobile smart devices, like smartphones, are increasingly used in several countries.

Since the above model is costly and inefficient both for users and SPs, the federated identity management (FIM) model has been proposed in the recent years [1]. In this model, the user registers his identity or profile with one organization (called Identity Provider—IdP), but he manages to get access to the services offered by various SPs without any further registration. User identities (or profiles) maintained by one organization can be trusted by another organization, provided the two organizations established a trust relationship, called also 'Circle of Trust' [2]. In the FIM model, upon successful authentication, IdP releases a security token to the user's agent (i.e., the browser), which forwards the token to SP by means of a FIM protocol.

As the number of IdPs and SPs increases, the trust relationships to be established and managed might become practically inefficient. For this scalability reason, but also for interoperability reasons in cross-border scenarios (e.g., when a smart card issued in one country by a government to their citizens is not automatically recognized in another country), it is helpful to have in place an interoperability platform composed of *national bridges*, which masks FIM implementation details to SPs and IdPs by providing a unified set of services in order to exchange user authentication data. Unlike the basic FIM model, SP does not directly contact IdP to authenticate the user, but contacts instead its own (national) bridge. On the other hand, the IdP receives user authentication requests and generates authentication responses for its own national bridge. This model is operational only if the two 'bridges' in the two countries can map and exchange data about the user authentication process in a transparent and secure manner.

The European pilot project STORK (Secure Identity Across Borders Linked) [3] and its follower STORK2 [4] created such a bridging system (or a pan-European electronic Identity Management architecture) to allow authentication means from one country to be accepted by applications in another European Union (EU) country (e.g., digital certificates from country X can be used to authenticate citizens in country Y). The STORK and STORK2 platforms were tested in several pilot use cases, e.g., for student mobility [5], for Wi-Fi access [6], or for digital certificate validation [7]. What lacked in STORK was the definition of clear liabilities and legal certainty in case of sensitive services, like in banking, financial, or health applications domains. However, the results and findings of the STORK project were used as baseline in the definition of the electronic IDentification, Authentication, and trust Services (eIDAS) Regulation [8], the STORK code has been exploited to build the eIDAS sample implementation [9], and the STORK protocol was used as starting point in the definition of the eIDAS technical specifications [10]. Today, many European countries have already set up eIDAS nodes (acting as national bridges) that are part of the eIDAS infrastructure and have performed eIDAS nodes conformance testing with the European Commission [11].

To authenticate persons and to provide (basic) attributes for them, the eIDAS nodes are connected to the national IdPs that are part of a notified eID scheme in that country. Germany, Italy, Belgium,

Spain, Estonia, and Croatia have already notified their eID schemes under eIDAS, while other countries are in the process of doing so. Many EU countries are currently adapting their national eIDAS node's interface to connect to the national eID scheme(s), in order to allow their citizens to authenticate in other countries by using authentication credentials issued by one of their notified IdPs. In Italy, an adaptation layer has been designed an implemented to connect the eIDAS infrastructure to the national digital identity system named SPID (Sistema Pubblico di Identità Digitale) [12], as part of the EU-funded project named FICEP (First Italian Cross-border eIDAS Proxy Service) [13].

Additionally, the eIDAS nodes have started to be connected to the national SPs to allow citizens to authenticate in their home country through the eIDAS infrastructure when accessing eIDAS-enabled services. However, the connection of Attribute Providers (APs) and SPs to the national eIDAS nodes and the development of new eIDAS services are still in their infancy [5,14]. This is due in part to the fact that sector-specific attributes (in domains like academia, business, eHealth) are not yet supported on the eIDAS nodes and thus cannot be transferred directly through the eIDAS framework. In other words, eIDAS is a horizontal legislation not entitled to one specific sector, in which the identification of persons and authentication part is distinguished from the provisioning of the attributes. Since the integration of the eIDAS nodes with the national APs is still an open issue, several research projects have started to work on this topic. For example, the eID4U project [15] explores the definition, the transport, and the retrieval of (new) academic attributes through the eIDAS nodes, as well as their usage in new eIDAS-enabled academic services involving universities from different countries. It is necessary that more and more universities offer degree programs in cooperation with other universities, but their student information systems (SIS) and learning management systems are still isolated [16]. We address such needs in our work by proposing real use cases exploiting the eIDAS federated authentication and attribute transfer to connect universities' SIS and build new services.

Contributions

We investigated the eIDAS infrastructure extension with support for the academic domain attributes and the development of new services exploiting such attributes. In practice, we will detail: (a) the definition of new academic and person attributes to be transferred through the eIDAS framework, as well as their support on the eIDAS node; (b) our approach used to retrieve the attributes from the IdPs and a separate AP through a so-called *AP Connector* module acting as adapter and attribute aggregator between the eIDAS node and specific national protocols for identity management and attribute retrieval; (c) the design, implementation, and installation in a controlled environment of two eIDAS-enabled services, eRegistration and eLogin, which exploit the eIDAS infrastructure to obtain the attributes in a reliable and fast way.

The paper is organized as follows: Section 2 gives an overview of the related work, Section 3 presents briefly the eIDAS infrastructure and attributes supported, Section 4 describes our approach to enable/support new academic and personal attributes in eIDAS, and Section 5 presents our proposed solution to retrieve and transfer (additional) academic attributes through the eIDAS interoperability framework. Section 6 details the eIDAS-enabled services eRegistration and eLogin services we have designed and implemented. Finally, Section 8 concludes the paper and indicates future work.

2. Related Work

Several research projects have worked on interconnecting identity federation technologies in different areas, like resilient data, biological information, or cloud services, some of which are resumed in [17]. In general, services are also continuously enriched with emerging technologies, e.g., development of Web-based technologies have driven the integration of e-commerce and social networks [18]. We discuss further below some European research projects in the academic area that are strongly related to our work, as we will spend part of our future work integrating our approach with these projects in a unified solution that can be used on one side by the universities to exchange

data for academic personnel securely and efficiently and, on the other hand, by the students and other academic personnel in new user-friendly services.

To transfer academic achievement results (e.g., transcript of records, diploma supplement, credits obtained for individual courses abroad), the EMREX project [19] designed and implemented a decentralized system composed of National Contact Points (NCPs) and also defined a specific format, named ELMO, which is based on XML (eXtensible Markup Language). Students may retrieve their academic achievements from a high education institution located in the same country or abroad through a dedicated application, named EMREX client. The academic results obtained by a student are digitally signed with the private key of the NCP that issued it.

EMREX does not define any authentication method but delegates this task to the university. When the student visits an university abroad, he/she will first register at the foreign university and get an authentication credential (e.g., a username/password) valid at the university abroad. When the student wants to transfer his academic records, he will be authenticated by means of that credential. In the long run, this is neither efficient nor secure: it is widely known that passwords can be attacked and, after some time, expire, thereby impeding the student to continue to correctly operate the academic achievement retrieval process. So, from this perspective, EMREX might be integrated in the future with eIDAS to allow student authentication in their home country. Moreover, if operational, EMREX could provide useful information for specific academic services orchestrated through eIDAS. For example, the transcript of records is a highly requested document in many academic services and an eIDAS-enabled academic service (like the eRegistration service described in the following) could be integrated with EMREX to allow for the transfer of such document.

In the European Student Card (ESC) project [20], students are provided with smart cards to be used for authentication, which contains a unique student European ID [21]. The idea to have a unique student European ID is good, as it could solve many problems encountered when trying to uniquely identify a student across EU. Since, at the moment, there is no such unique identifier largely adopted across EU, multiple workarounds or alternatives need to be implemented in cross-border scenarios to uniquely identify persons. For example, in the eLogin service described further below, we study some possible solutions. Allowing students to benefit from new services (e.g., reductions at the libraries or at university restaurant) only at the universities that voluntarily adhered to the project and thus recognize the (university) card is the main limitation in ESC.

Erasmus Without Paper (EWP) project [22] instead focused on services for Erasmus student mobility. EWP allows universities to implement an end-to-end process of paperless student exchange, as well as documents related to student mobility. EWP basically defined an EWP network to enable the exchange of student data in an electronic format (directly) between institutions and implemented some applications required in student mobility, e.g., the Erasmus+ Dashboard allowing incoming and outgoing students to manage, sign, and review their online learning agreements and to communicate with partner institutions. This feature might then be integrated with eIDAS-enabled eRegistration service proposed in the following because the learning agreement is a document required in our service, but we do not foresee transferring it through eIDAS.

The eduGAIN (EDUcation Global Authentication INfrastructure) project set up a framework that connects research and education organizations and is operating with impressive numbers, e.g., nearly 2600 IdPs and 1800 SPs [23]. eduGAIN has started as part of the project GÉANT (2004–2009), co-funded by the European Commission and, more recently, is part of the GÉANT 2020 Framework Partnerhip Agreement. In addition to the IdPs and to the SPs, the eduGAIN framework contains also a Discovery Service (DS) to allow a user to choose their home organization, where they will be authenticated, and a Metadata Distribution Service (MDS), which contains technical and descriptive details about the SPs and IdPs. eduGAIN uses Shibboleth [24] and SAML 2.0 protocol [25] with no extensions (e.g., no extension is defined for the quality of attributes). Even though it is based on SAML, eduGAIN uses a different identifier and a different message format with respect to eIDAS. A proposal aimed to interoperate the eduGAIN with STORK is given in [17].

3. eIDAS Infrastructure in Brief

The eIDAS interoperability framework comprises two different authentication models. In the *proxy model*, each country adhering to this model has to run a single national bridge called *eIDAS node*. This element is actually composed of two logical subcomponents: an eIDAS-Proxy-Service (in short, eIDAS Proxy), which is in charge of communicating with the National eID scheme to which the citizen will be authenticated; and one eIDAS-Connector (in short, Connector), which is in charge of communicating with the national SPs. Note that it is possible to have more than one Connector; for example, in Italy there is a "public" Connector that is used to provide public eIDAS-enabled services and a "private" Connector that may be exploited for private eIDAS aware services. The *middleware model* (adopted by Germany) does not exploit a national bridge: the eIDAS Connector (in the other countries) communicates with a country-specific Middleware-Service (MW) to allow SPs to provide eIDAS-enabled services to German citizens. Citizen authentication is delegated from an SP to its national Connector, which acts as a gateway and subsequently forwards the authentication request to the eIDAS Proxy of the country selected by the citizen (or to the MW), as shown in Figure 1. The authentication request is further handled by the eIDAS Proxy according to Member State (MS)-specific approach. Most countries follow the traditional approach, in which a new authentication request is constructed by the eIDAS Proxy and is sent (through the user's browser) to the national IdP (part of the National eID scheme). At the IdP, the citizen is asked to authenticate with a national eID. If this operation completes successfully, an authentication response containing also the eIDAS attributes that have been requested are returned through the eIDAS infrastructure back to the requesting SP.

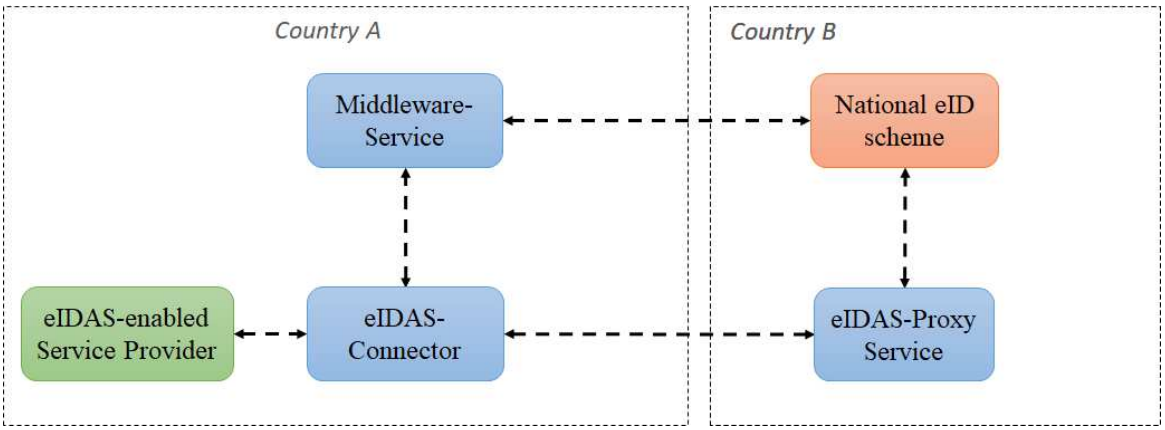

Figure 1. Electronic IDentification, Authentication, and trust Services (eIDAS) architecture.

Each eIDAS node has a *Specific* part used to communicate with the national SPs and IdPs and a *Generic* part used to communicate with the other eIDAS nodes via the eIDAS communication protocol [26]. Such protocol is based on SAML 2.0 WebSSO Profile [27] to transfer authentication data and eIDAS attributes between the eIDAS nodes.

Attributes for Natural Persons

According to the eIDAS specification, the eIDAS nodes may exchange only a restricted set of personal attributes, named *eIDAS minimum data set (MDS) for natural persons*, containing the person's current family name(s), the current first name(s), the date and place of birth, an eIDAS unique identifier, the current address, and the gender of a person. The attributes are either mandatory (i.e., the eIDAS unique identifier, the current family name(s), the current first name(s) and the date of birth) or optional (the place of birth, the current address and the gender). We note an important aspect: We need to distinguish the set of attributes "mandatory" for eIDAS (the attributes mentioned above) and the set of attributes considered "mandatory" for the eIDAS-enabled SP in order to provide a service. For example, the number of a person's health insurance card or even their marital status could be

considered mandatory in some SP. Note also that there is some ambiguity for the place of birth (typically it contains the town of birth), while other attributes often required (e.g., nationality, citizenship or even information about the identification document of a citizen) are not defined in the eIDAS specification, as they are considered sector-specific attributes.

4. Definition and Support for New Attributes in eIDAS

To develop the proposed eIDAS-enabled services, we defined first the attributes needed by the services. Some academic attributes typically required to register a foreign student as an Erasmus student at a visiting university or the home student's university name (and its Erasmus code), and the course in which a student is currently enrolled in their university. Other additional attributes are specific to the Erasmus program, such as the contact person at the international Erasmus office (his address, fax, phone number, email) or the academic advisor of the student at their home university (along with their address, faculty name of the academic advisor, and their phone and email address).

Thus, we have divided the attributes in three sets: the personal ones, the academic ones, and the program-specific ones. The personal attributes contain data used to identify a person, so in this set we can include the eIDAS *MDS* for natural person attributes, plus some other additional attributes, such as data about the identification document (passport or identity card), like the `ID Number`, `ID issued by` or `ID expiration date`. The academic attributes contain data about the academic career of a student, such as the `country of study`, the `university name`, `the field/area of study`, and the `level` (e.g., undergraduate, graduate, PhD). The program-specific attributes are required by specific study programs, such as the `period of stay` or the `proposal of learning agreement (study plan)`. In our approach, these attributes will not be transferred through eIDAS, but they will be communicated through other means; for example, they might even be self-declared by the student directly on the university's dedicated portal.

Enabling Academic Attributes on the eIDAS Node

The new attributes were added to the eIDAS code [9], resulting in a new version called eID4U eIDAS code [28]. We have installed the eID4U eIDAS code in an experimental testbed that hosts a dedicated academic eIDAS node acting both as eIDAS Connector and as eIDAS-Proxy Service, as shown in Figure 2. This environment is deployed by using a Docker infrastructure [29] running on an Ubuntu Server 16.04 virtual machine hosted at Politecnico di Torino.

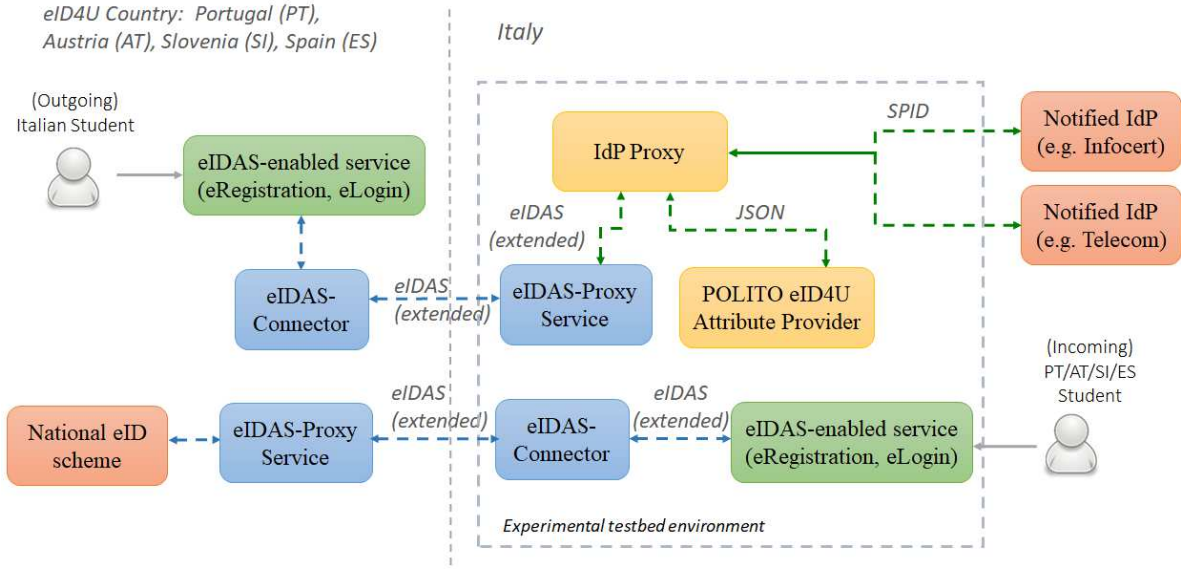

Figure 2. Experimental testbed hosting the eIDAS node extended with support for new attributes, connected to notified Identity Providers (IdPs) and an academic Attribute Provider (AP).

Today, the official Italian eIDAS node is managed in Italy by the Agenzia Nazionale per l'Italia Digitale (AgID), in the frame of the FICEP project. Actually, the Italian eIDAS code is handled (compiled, deployed, tested) in three deployment environments. The test environment is used for development, and it is only available for internal use. The quality assurance (QA) is used to check the interoperability with other MSs before going into production and is linked to notified IdPs in Italy issuing SPID authentication credentials to (real) users. The production environment represents the real Italian eIDAS Node.

Originally, we derived our experimental testbed from the one used for the official Italian eIDAS test environment established in the FICEP project. Thus, each eIDAS node component starts in its own docker container, using Apache Tomcat application server [30]. Additionally, other modules specific to the Italian eIDAS infrastructure also start in their own docker container, such as the reverse proxy (based on HAProxy [31]) and the IdP Proxy. Next, we have extended the experimental testbed to host also the application (called POLITO eID4U Attribute Provider), which is currently used for attribute retrieval of academic attributes from our university (further detailed in Section 5). Moreover, the experimental testbed hosts also the eIDAS-enabled services, further detailed in Section 6.

The components of the eIDAS node in the experimental testbed are accessible via TLS protocol [32]. The digital certificates for all the node components in the testing environment are issued by Let's Encrypt [33]. The full list of Domain Name Servers (DNS) names of all the components in the experimental testbed is shown in Table 1.

Table 1. Domain Name Servers (DNS) names of components in the experimental testbed.

Component	Testing Environment URL
eIDAS-Proxy Service	`service-test-eid4u.polito.it`
eIDAS-Connector	`connector-test-eid4u.polito.it`
IdP Proxy	`idp-proxy-test-eid4u.polito.it`
POLITO eID4U AP	`demo-ap-test-eid4u.polito.it`
eIDAS-enabled eRegistration for Erasmus students	`apply-eid4u.polito.it`
eIDAS-enabled eLogin	`login-eid4u.polito.it`

5. Integration of the eIDAS Node with the Academic APs

5.1. The Proposed AP Connector Module

The current eIDAS code released by the European Commission [9] allows the selection of the country in which the citizen will be authenticated and the eIDAS attributes for him/her will be obtained. However, if additional (sector-specific) attributes need to be transferred, the code does not allow to select the AP(s) from where such attributes may be retrieved. This is due to the fact that the attribute retrieval is considered MS specific, i.e., each country may design and implement its own solution for (sector-specific) attribute retrieval. In the countries where the national eID infrastructure does not provide other new attributes in addition to the eIDAS attributes for natural persons, a new function on the eIDAS node to allow the selection of the AP from which to retrieve the attributes should be added. Basically, if an eIDAS node needs to value both the eIDAS *MDS* attributes and other additional attributes, either it gets them directly from the national eID infrastructure or it has to employ an additional service or module. In the eID4U project, we proposed the AP Connector module illustrated in Figure 3. This module is considered *optional* because in some countries the national infrastructure could directly provide the additional attributes to the national eIDAS node, e.g., the ones running a centralized platform for citizen's electronic identity and attribute management.

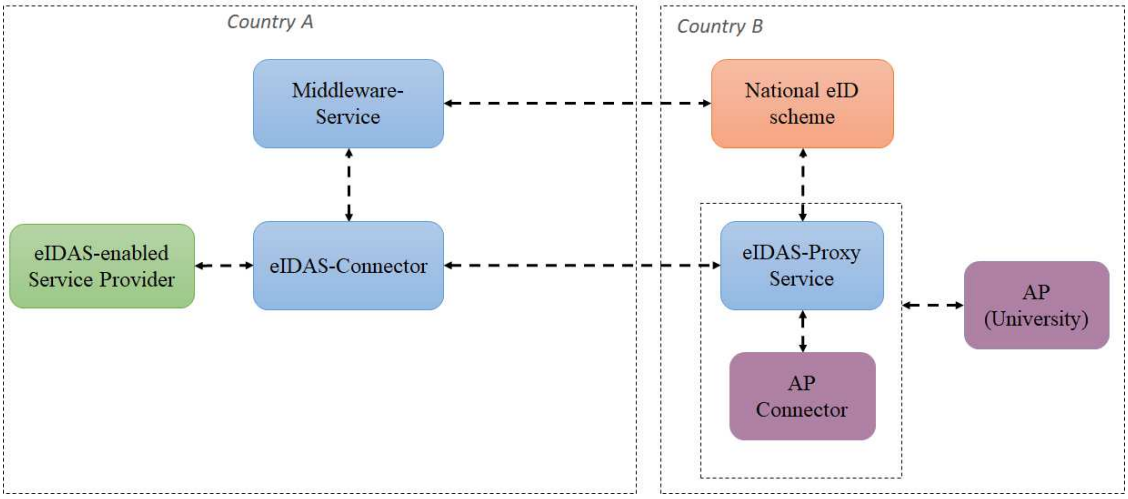

Figure 3. The proposed AP Connector module employed for additional attribute retrieval from the national specific AP(s).

In other countries, the IdPs issuing authentication credentials and also providing some personal attributes are separate from the APs providing other domain specific attributes. For example, in the eID4U project, the APs are universities that typically already have a system in place for management of academic personnel (students, teachers) and for handling their academic attributes (e.g., academic career, courses followed, and credits obtained). The universities also have systems in place that allow them to federate services inside the university or with other partners. For example, some of them have adopted Shibboleth [24], which is a SAML based open-source framework, while others are in the process of installing or running other similar systems. Other universities may even be connected to national system connecting the APs in a specific domain (in our case, academic domain).

The AP Connector module acts as adapter between the eIDAS node and the AP running specific protocol(s) for academic attribute exchange. The AP Connector would be exploited in the following scenarios: (1) when the national eID scheme/infrastructure in a country does not provide the additional requested attributes together with the eIDAS attributes for natural persons; (2) if an AP does not have a specific solution for mapping/filtering the academic attributes from AP specific format to/from eIDAS format.

5.2. AP Connector Implementation

We have implemented the AP Connector module by extending the *IdP Proxy* component, which is part of the adaptation layer that links the Italian SPID system to the eIDAS infrastructure. The IdP Proxy performs several tasks, such as allowing selection of which (notified) IdP the citizen will use for authentication, and it converts the authentication request and response messages from the eIDAS format to/from the SPID format supported by the notified IdPs. In our implementation, the academic attributes are retrieved from the Politecnico di Torino (acting as AP). In Italy, almost all databases storing citizen data are indexed based on the citizen's fiscal number (in Italian, codice fiscale). However, the fiscal number is not part the eIDAS *MDS* for natural persons. So, we modified the IdP Proxy to also retrieve the fiscal number from the notified IdPs in addition to the attributes that are part of the eIDAS *MDS*, even though the (foreign) SP has not asked for it, as shown in Algorithm 1. Once the fiscal number is returned from the IdP, the IdP Proxy (through the AP Connector module) sends it to the POLITO eID4U AP application, which returns the requested attributes (in JSON format [34]) for the person with that fiscal number. When the fiscal number is used for attribute retrieval (so it has not been actually requested by an SP), its value is filtered when the valued attributes are sent from the back to the eIDAS node. The IdP Proxy constructs the overall authentication response message

(in eIDAS format) containing both the attributes collected from the IdP and the ones from the AP, which is further passed to the eIDAS Proxy Service.

Algorithm 1 AP Connector algorithm used to retrieve attributes from an IdP and an AP based on a national person identifier shared among IdP and AP, e.g., the fiscalNumber.

```
requestedAttributes ← getAttributesFromSAMLRequest()      ▷ Request received from eIDAS node
for all attribute ∈ requestedAttributes do
    if attribute ∈ IdPAttributes then
        IdPRequest ← IdPRequest + attribute                ▷ List of attributes to request to IdP
    end if
end for
if IdPRequest ≠ requestedAttributes then                   ▷ Some attributes are provided by the AP
    if fiscalNumber ∉ IdPRequest then
        IdPRequest ← IdPRequest + fiscalNumber             ▷ Add fiscalNumber request if missing
    end if
end if
IdPResponse ← getAttributesFromIdP(IdPRequest)             ▷ Retrieve attributes from IdP
for all attribute ∈ requestedAttributes do
    if attribute ∉ IdPResponse then
        APRequest ← APRequest + attribute                  ▷ List of attributes to request to AP
    end if
end for
if fiscalNumber ∈ IdPResponse then
    fn ← getFiscalNumber(IdPResponse)
    APResponse ← getAttributesFromAP(APRequest, fn)        ▷ Retrieve attributes from AP
    if fiscalNumber ∉ requestedAttributes then
        IdPResponse ← IdPResponse − fiscalNumber           ▷ Remove fiscalNumber if not requested
    end if
end if
sendSAMLResponse(IdPResponse, APResponse)                  ▷ Send SAML response to eIDAS node
```

6. Proposed eIDAS-Enabled Academic Services

6.1. eIDAS-Enabled eRegistration Service

6.1.1. Service Description

The students' registration service is one of the most widely used at universities. Since more and more students study abroad for short or long terms, we have proposed the eRegistration for (incoming) Erasmus students to be integrated with the eIDAS infrastructure, but our proposal works fine and can be extended easily to handle also student registration in other study programs at our university (e.g., bachelor, master).

At present, the incoming Erasmus students perform registration procedures at our university through the web portal, where they provide some personal data, which has to be inserted manually and has to be verified subsequently by the operators. The initial page accessed by an Erasmus student is available at http://apply.polito.it, where in a dedicated web form, the student provides first a set of personal data, such as Family name, First name, Country of birth, Birthplace, Date of birth, Gender, Citizenship, Email address, and data about the Identity document, Current, and Temporary address. Note that the Email address is used as a kind of person identifier because upon selection of eligibility of a student for the Erasmus program, all subsequent internal procedures for a student are associated with the email address the student has chosen to be used during their Erasmus mobility.

Once the student has provided all the personal data, an account/profile is created for them in the university system, and they can get access with a username and password. In order to complete the registration, the student has to access their account/profile, and they have to provide additional information, as required by the Erasmus application [35], such as the transcript of records, a proposal of learning agreement (study plan), copy of passport or ID card (EU citizens), program mobility data, such as the period of stay (e.g., three months), the home institution data (including the contact person at the International office and the academic advisor), certification stating the Italian and English language proficiency, and so on. Note that most of this information is *self-declared*: The student fills most of these fields in the dedicated area and uploads (as attachments) files containing scanned copies of their passport or ID card, about their academic career, language certificates obtained, or about the confirmation of their status as an exchange student. In brief, many parts of the administrative procedure for the Erasmus registration are still paper-based, although a friendly Web-based interface exists that allows the uploading of scanned copies of the official documents, which will be subsequently verified by the personnel at the International office.

In the eIDAS-enabled eRegistration service, some attributes about the academic career of the student are retrieved through the eIDAS infrastructure in addition to the ones regarding the identity of the student, including the eIDAS attributes for natural persons, e.g., name, surname, date of birth. Examples of additional academic attributes required by this service are: the university at which the student is currently enrolled, as well as the course name and the field and level of study. Since the Erasmus offices obtain the data required for registration or pre-registration of incoming students through the eIDAS network, they would perform the registration procedure much faster, reducing thus the number paper documents to be processed and the manual insertion/verification of the data.

6.1.2. Implementation Details

In the first stage, we have defined new *service-oriented attributes*, as introduced first in [36] and resumed in Section 4. The set of personal attributes requested for this service at our site are shown in Table 2, while the academic ones are shown in Table 3. The program-specific attributes (like the learning agreement or the contact person at the international office) are not expected to be transferred through eIDAS node. The whole set of newly defined attributes for a natural person can be seen in a test SP application we have installed at https://demo-sp-test-eid4u.polito.it/SP/populateIndexPage, under the eid4u namespace, e.g., `Citizenship` (representing the citizenship) or `homeinstitution/Identifier` (representing the identifier of the home university of a student).

In the second stage, in order to support the (outgoing) Italian students that have to register at foreign universities, we have linked the eIDAS node to two IdPs, namely Infocert and TIM Telecom Italia, which have notified their eID schemes under eIDAS. Basically, these IdPs issue authentication credentials to citizens and implement the SPID protocol (which is SAML-based) [37] that has to be supported by public bodies and may be supported by private organizations to implement federated services in Italy. To communicate with the IdPs, the eIDAS Proxy contacts an adaptation layer (i.e., IdP Proxy) that converts the eIDAS messages to SPID protocol, as shown in Figure 2. Note that the IdP Proxy is seen as an IdP from the eIDAS node's perspective. In fact, the IdP Proxy owns its own SAML metadata, and it is in a circle of trust with the eIDAS node (on one side) and with the SPID-aware IdP (on the other side). In the future, the IdP Proxy may run as a service hosted by a dedicated service vendor, separately from the eIDAS node. Security concerns, such as preventing data from unexpected usage on the remotes [38], could be addressed in the IdP Proxy.

Table 2. Personal attributes defined in eID4U for Erasmus eRegistration at our university, with indication of mandatory (M)/optional (O).

SAML Attribute Name		**Description**
Name in eID4U	**M/O**	
(eIDAS) Person Identifier	M	Unique identifier of a natural person in eIDAS
(eIDAS) Current First Name(s)	M	Given name(s) of a natural person
(eIDAS) Current Family Name(s)	M	Family name(s) of a natural person
(eIDAS) Date Of Birth	M	Date of birth of a natural person
(eIDAS) Gender	M	Gender
(eIDAS) Current Address	M	Current address of a natural person
(eIDAS) Place of Birth	M	City of birth of a natural person
Temporary Address	M	Temporary address of a natural person
Email	M	Mail of a natural person
Phone	M	Phone number of a natural person
Id type	M	Identification document type (National identity or passport)
Id number	M	Identification document number
Id expiration date	M	Expiration date of the identification document
ID issued By	M	Entity that issued the identification document
EU health card ID	O	European health insurance card of a natural person
Nationality	O	Nationality of a natural person
Citizenship	M	Citizenship of a natural person
Marital state	O	Marital state of a natural person
Country of birth	M	Country of birth of a natural person
Current photo	O	Current photo of a natural person
Tax identification Number	M	Fiscal tax identification number of a natural person

Thus, as explained in Section 5.2, we modified the IdP Proxy to retrieve additional attributes (i.e., the ones not valued by the IdP) from the AP of Politecnico di Torino, which we implemented as an ad-hoc application. The retrieval of the additional attributes is based on the national identifier, namely the student's fiscal number (in italian, codice fiscale), which is provided at birth to any Italian citizen (and is persistent throughout their life) and is assigned to foreign citizens that work and study in Italy.

In the third stage, we integrated the new application implementing the eIDAS-enabled Erasmus eRegistration on the web portal of the university. To do so, we created an eIDAS-enabled application allowing the selection of the initial personal attributes that are required also in the original Erasmus registration form, as illustrated in Figure 4. After the selection of the citizen country, an authentication request in eIDAS format extended with support for new attributes is constructed and is sent to the eIDAS Connector and subsequently it is forwarded to the (selected country's) eIDAS Proxy. Assuming that the authentication in the foreign country and the retrieval of the requested (personal) attributes proceeds correctly, the returned valued (personal) attributes are shown in a web page as illustrated in Figure 5. Next, by clicking "Register", they are stored in a student profile created in the university's information system. Since some of the academic attributes might not be valued, the student has the possibility to login (note the button in the upper right area of the page) with eIDAS credentials in addition to the (university) credentials (username/password) that they created in the previous step. Once the student is logged-in, they have access to a dedicated area where they can retrieve values from their home university for some (individual) attributes by exploiting eIDAS (e.g., for the copy of their passport or for the current photo), or they can upload some scanned documents (such as for the diploma supplement or for transcript of records).

Table 3. Academic attributes defined in eID4U for Erasmus eRegistration at our university, with indication of mandatory (M)/optional (O).

SAML Attribute Name		Description
Name in eID4U	**M/O**	
Home institution	M	Name and Erasmus institutional code of the sending higher educational institution
Country of the home institution	M	Country of the sending higher educational institution
Address of the home institution	M	Full address of the sending higher educational institution
Current level of study	M	Current level of study of the student, defined by an ISCED level code
Current field of study	M	Current field of study of the student, defined by an ISCED code
Current degree name	O	Name of the degree the student is currently pursuing in their studies
Transcript of records	M	The signed and stamped document confirms the student's current academic status and details the curricular units obtained so far by the student at the sending higher educational institution.
Degree	M	The highest previous student's education completed, defined by qualification level (as an ISCED level code), the degree name, and the final and average grade
Year of graduation	M	Year when the student received their last obtained degree
Degree country	M	Country where the student received their last obtained degree
Level of language proficiency	M	Declaration of level of (English) language knowledge
Language certificate	M	Certificate of language knowledge

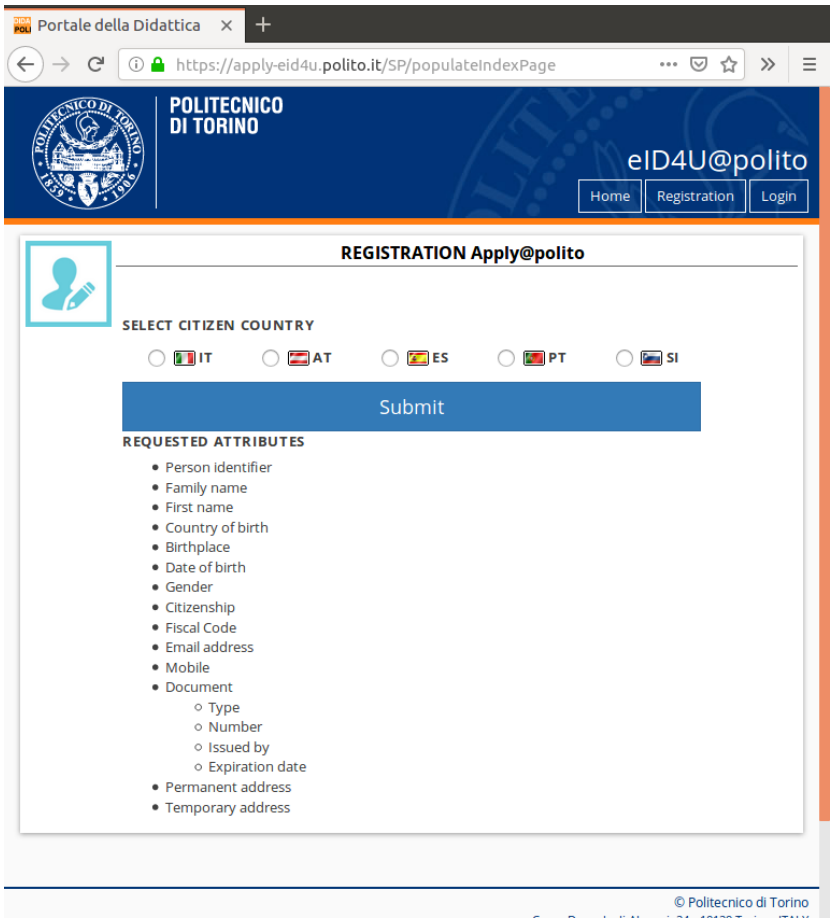

Figure 4. Initial Erasmus registration form enabled with eIDAS infrastructure.

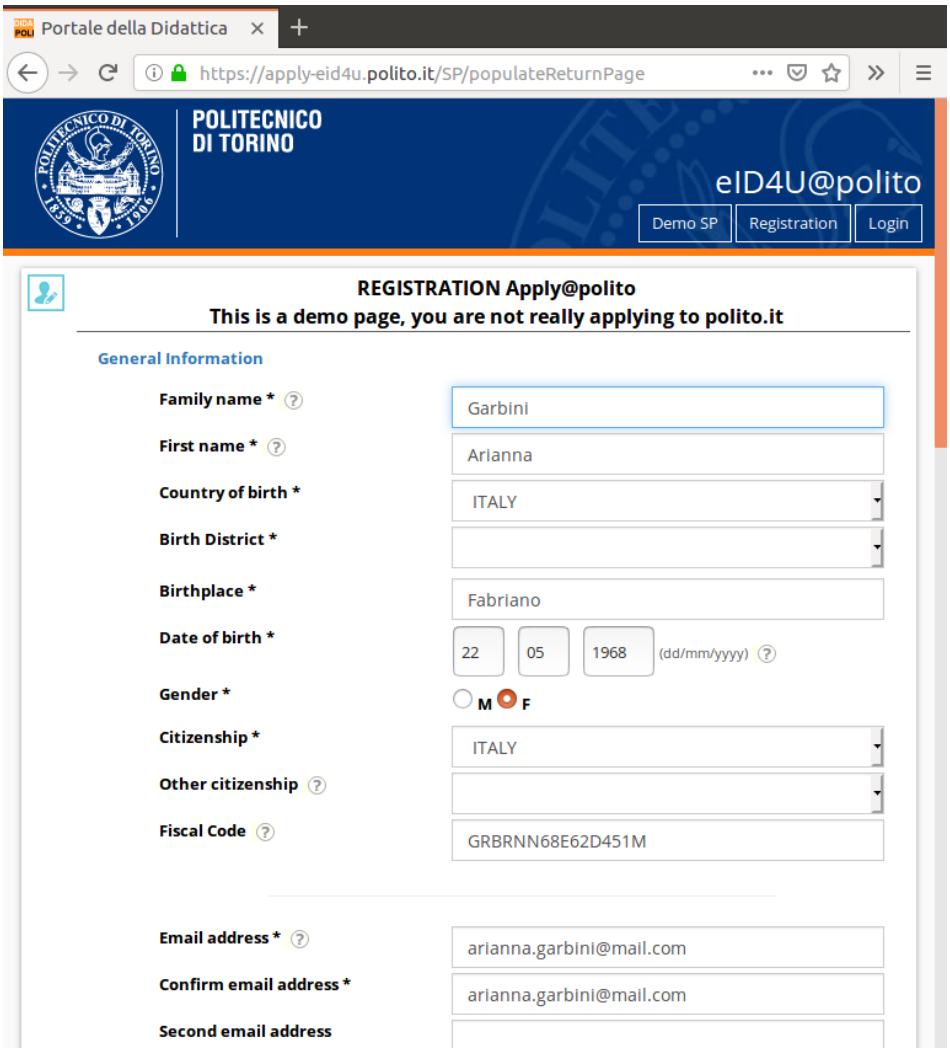

Figure 5. Erasmus registration form populated with data retrieved through eIDAS infrastructure.

6.2. eIDAS-Enabled eLogin Service

6.2.1. Service Description

Universities have already in place a single sign-on system allowing their users to authenticate once with the credentials issued by the university (e.g., a username and password or with a soft X.509 certificated stored in the browser with a hard X.509 certificate stored on a smart card) and then transparently get access to several services. In our university, Italian students are also allowed to login on the portal with their national SPID credentials, issued by SPID-aware IdPs. The Login is typically offered after the student has registered at that university. In addition, to allow access to restricted resources, such as to distance learning courses to persons that are not currently enrolled in the university but have to be authenticated, one possibility could be to exploit the proposed eIDAS-enabled eLogin.

Moreover, some existing services at the university could be enhanced by incorporating the strong authentication that can be performed through eIDAS infrastructure. For example, many services on the university portal are typically accessed through university credentials, like a username and password. The password loss is a problem often encountered nowadays: the users forget their university credential (i.e., the password), and they have to contact a Help Desk for recovery. The eIDAS-enabled eLogin could be helpful in this case of password loss: the person (student, teacher, or administrative personnel) could be asked to perform strong authentication through the eIDAS infrastructure (with their national eID)

and, upon successful completion of eIDAS-enabled eLogin, they would be able to automatically recover their university credentials, reducing (or even avoiding) the contact with the university's helpdesk.

6.2.2. Implementation Details

The set of personal attributes relevant for this service are the ones that are part of the eIDAS *MDS* for natural persons. The lack of a unique identifier for a student across EU is the most challenging issue in this service. In eIDAS, an (eIDAS) person identifier has been defined but this is not single value (i.e., a citizen may have two different eIDAS personal identifiers in two different IdPs, depending on which one they are using for authentication, as is the case in Italy) and may change in time (e.g., it may change after five years). This fact influenced the implementation of this service. When a student chooses to login with eIDAS, they are presented with an initial page in which the personal attributes indicated in Table 4 are requested. Then, they are redirected through the eIDAS infrastructure in their home country where they can be authenticated with national credentials. Upon authentication, the above set of attributes are returned through the eIDAS infrastructure back to the eLogin application. To check if the (foreign) student that has been authenticated is also registered in our university database, first the eLogin application makes a search based on the eIDAS person identifier, assuming that the student has linked/stored his identifier(s) to his profile in the university database. If such identifier is not found, the eLogin application makes a search based on the returned values of the eIDAS *MDS* attributes for natural persons. However, since this set of values alone might not be sufficient to uniquely identify a student, an additional step has to be taken be the university to resolve ambiguities (e.g., two persons with the same name surname and date of birth might be registered in the internal database). In this case the student could be asked, for example, to provide some more additional information (e.g., their national document identification type and number, like a passport number) and the provided data would be compared to the one retrieved through eIDAS.

Table 4. Personal attributes requested for Login with eIDAS, with indication of mandatory (M)/optional (O).

SAML Attribute Name		**Description**
Name in eID4U	**M/O**	
(eIDAS) Person Identifier	M	Unique identifier of a natural person in eIDAS
(eIDAS) Current First Name(s)	M	Given name(s) of a natural person
(eIDAS) Current Family Name(s)	M	Family name(s) of a natural person
(eIDAS) Date Of Birth	M	Date of birth of a natural person
(eIDAS) Gender	M	Gender
(eIDAS) Place of Birth	O	Place of birth of a natural person

7. Implications

We are currently in the process of migrating the modifications done on the eIDAS node and on the IdP Proxy in our experimental testbed to the official eIDAS node in QA environment hosted and managed in Italy by AgID. This implies that the official eIDAS node itself will be changed to accommodate the newly defined attributes. The official IdP Proxy will also be changed with the one created to retrieve additional attributes from the AP. Note also, the SAML metadata configured on the IdP Proxy (containing IdP URLs, certificates, and attribute sets that may be exchanged between the IdP Proxy and the SPID-aware IdP) will have to be adapted since the fiscal number will be requested from the SPID-aware IdPs, in addition to the eIDAS MDS for natural persons.

At the same time, we will connect the eRegistration and eLogin services at our site to the official eIDAS node, giving us the possibility to validate in the future the services with real users that will use their SPID credentials (e.g., username and password) in accessing the proposed services.

In terms of performance, authors in [39] evaluated the eIDAS architecture in local, organizational, and remote environments. They measured the average time needed for a user identification after they

have been identified at least once, which means that the cache of the eIDAS node is storing some data for the user during some time period. They showed it took: about 1 s to authenticate a user through eIDAS in local and organizational environment, i.e., when the eIDAS node and the clients were on the same node; 2.5 s to authenticate a user in federated EU nodes, i.e., eIDAS nodes in Germany and Spain, where the average network latency was 20 ms; 9 s to authenticate a user in a federated environment in Mexico, i.e., eIDAS nodes in Mexico and Spain, where the average network latency was 120 ms. This study does not consider additional steps to be performed for retrieving additional attributes.

8. Conclusions and Future Work

Building an efficient and scalable eIDAS infrastructure requires, at the European level, the integration and harmonization of several systems that were originally designed, implemented, and maintained by different entities, with different tools and approaches. For example, the national governments or public agencies basically operate the eIDAS node(s), and the eID systems are managed by public or private IdPs (recognized through mechanisms specific to each country) connected to the eIDAS node(s), while the sector-specific attributes, like the academic ones, are provided by the universities.

In this paper, we proposed and implemented the integration of academic attributes into the eIDAS infrastructure to support some cross-border academic services. We detailed our solution for academic attribute retrieval, as well as the design for implementation of two eIDAS-enabled services largely used by the students: the eRegistration to the Erasmus student mobility program and the eLogin on the university's web site.

Future work includes the evolution of our AP towards an AP Proxy that will support multiple APs (potentially from different universities) and will handle this conversion of different attribute formats to/from eIDAS format.

Author Contributions: Conceptualization, D.B. and A.L.; Funding acquisition, D.B. and A.L.; Investigation, D.B., A.L. and C.C.; Project administration, D.B. and A.L.; Software, D.B. and C.C.; Supervision, A.L.; Validation, D.B. and C.C.; Writing—original draft, D.B.; Writing—review & editing, D.B., A.L. and C.C.

Funding: This work was developed in the framework of the eID4U project, co-funded by the European Union's Connecting Europe Facility, Call for proposals: CEF Telecom Call 2017, Proposal Code: 2017-EU-IA-0051, under the grant agreement no. INEA/CEF/ICT/A2017/1433625.

Acknowledgments: Authors would like to thank Giorgio Santiano from Politecnico di Torino and Paolo Smiraglia from Agenzia Nazionale per l'Italia Digitale (AgID) for their help and feedback in integrating the solution proposed in this paper with the Student Service Office of Politecnico di Torino and with the official Italian eIDAS node, hosted by AgID.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Torres, J.; Nogueira, M.; Pujolle, G. A survey on identity management for the future network. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 787–802. [CrossRef]
2. Malik, A.A.; Anwar, H.; Shibli, M.A. Federated identity management (FIM): Challenges and opportunities. In Proceedings of the 2015 Conference on Information Assurance and Cyber Security (CIACS), Rawalpindi, Pakistan, 18 December 2015; pp. 75–82. [CrossRef]
3. Hernandez-Ardieta, J.L.; Heppe, J.; Carvajal-Vion, J.F. STORK: The European electronic identity interoperability platform. *IEEE Lat. Am. Trans.* **2010**, *8*, 190–193. [CrossRef]
4. Secure Identity Across Borders Linked (Stork) 2.0 Project (2012–2015). Available online: https://ec.europa.eu/digital-single-market/en/content/stork-take-your-e-identity-you-everywhere-eu (accessed on 10 June 2019).
5. Berbecaru, D.; Lioy, A.; Mezzalama, M.; Santiano, G.; Venuto, E.; Oreglia, M. Federating e-identities across Europe, or how to build cross-border e-services. In Proceedings of the AICA-2011: Smart Tech and Smart Innovation conference, Torino, Italy, 15–17 November 2011; 10p. Available online: http://security.polito.it/doc/public/torsec_aica2011_stork.pdf (accessed on 10 June 2019).

6. Berbecaru, D.; Lioy, A.; Aime, M.D. Exploiting Proxy-Based Federated Identity Management in Wireless Roaming Access. In *Trust, Privacy and Security in Digital Business (TrustBus 2011)*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2011; Volume 6863, pp. 13–23. [CrossRef]
7. Berbecaru, D.; Lioy, A. Exploiting the European Union trusted service status list for certificate validation in STORK: Design, implementation, and lessons learnt. *Softw. Pract. Exp.* **2015**, *45*, 1457–1477. [CrossRef]
8. *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/ec*; European Union: Brussels, Belgium, 2014.
9. eIDAS-Node Software Releases. Available online: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eIDAS-Node+Integration+Package (accessed on 10 June 2019).
10. eIDAS Technical Specifications v1.1. Available online: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2016/12/16/eIDAS+Technical+Specifications+v.+1.1 (accessed on 10 June 2019).
11. eIDAS Conformance Testing. Available online: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Testing+-+eID+Interoperability+Readiness+Testing (accessed on 10 June 2019).
12. Sistema Pubblico di Identità Digitale. Available online: https://www.spid.gov.it/ (accessed on 10 June 2019).
13. FICEP—First Italian Cross-border eIDAS Proxy Server. Available online: https://www.agid.gov.it/it/piattaforme/eidas/progetto-ficep (accessed on 10 June 2019).
14. Berbecaru, D.; Lioy, A. On the design, implementation and integration of an Attribute Provider in the Pan-European eID infrastructure. In Proceedings of the IEEE Symposium on Computers and Communication (ISCC), Messina, Italy, 27–30 June 2016; pp. 1263–1269.
15. eID4U Project—eID for University (2018–2019). Available online: https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/2017-eu-ia-0051 (accessed on 10 June 2019).
16. Boehringer, D. eLearning infrastructures for co-operative degree programmes in Europe. In Proceedings of the IEEE Global Engineering Education Conference (EDUCON), Tallinn, Estonia, 18–20 March 2015; pp. 73–76. [CrossRef]
17. Torroglosa, E.; Ortiz, J.; Skarmeta, A. Matching federation identities, the eduGAIN and STORK approach. *Future Gener. Comput. Syst.* **2018**, *80*, 126–138. [CrossRef]
18. Gai, K.; Qiu, M.; Sun, X. A survey on FinTech. *J. Netw. Comput. Appl.* **2018**, *103*, 262–273. [CrossRef]
19. The EMREX Project. Available online: http://emrex.eu/ (accessed on 10 June 2019).
20. European Student Card project. Available online: http://europeanstudentcard.eu (accessed on 10 June 2019).
21. European-Student-Card-Specifications. Available online: http://europeanstudentcard.eu/wp-content/uploads/2017/02/2017_03_21_European-student-card-Specifications-v1.pdf (accessed on 10 June 2019).
22. Erasmus without Paper project. Available online: https://www.erasmuswithoutpaper.eu/ (accessed on 10 June 2019).
23. eduGAIN Official Website. 2019. Available online: https://edugain.org/ (accessed on 10 June 2019).
24. Shibboleth. Available online: http://www.internet2.edu/products-services/trust-identity/shibboleth/ (accessed on 10 June 2019).
25. Cantor, S.; Kemp, J.; Philpott, R.; Maler, E. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard. March 2005. Available online: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf (accessed on 10 June 2019).
26. eIDAS SAML Message Format, Version 1.1. Available online: https://ec.europa.eu/cefdigital/wiki/download/attachments/80183964/eIDAS%20Message%20Format_v1.1-2.pdf?version=1&modificationDate=1497252919575&api=v2 (accessed on 10 June 2019).
27. Hughes, J.; Cantor, S.; Hodges, J.; Hirsch, F.; Mishra, P.; Philpott, R.; Maler, E. Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard. March 2005. Available online: http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf (accessed on 10 June 2019).
28. eIDAS-Node. Available online: https://github.com/eID4U/eIDAS-node (accessed on 10 June 2019).
29. Docker—Build, Ship and Run Any App, Anywhere. Available online: https://www.docker.com (accessed on 10 June 2019).
30. Apache Tomcat. Available online: http://tomcat.apache.org/ (accessed on 10 June 2019).
31. HAProxy. Available online: http://www.haproxy.org/ (accessed on 10 June 2019).
32. Rescorla, E. The Transport Layer Security (TLS) Protocol Version 1.3. 2018. Available online: https://tools.ietf.org/html/rfc8446 (accessed on 10 June 2019).

33. Let's Encrypt. Available online: https://letsencrypt.org/ (accessed on 10 June 2019).
34. JavaScript Object Notation. Available online: http://json.org/ (accessed on 10 June 2019).
35. Students Exchange Application Form. Available online: http://international.polito.it/admission/exchange_programmes/students_exchange_application_form (accessed on 10 June 2019).
36. Berbecaru, D.; Lioy, A. On integration of academic attributes in the eIDAS infrastructure to support cross-border services. In Proceedings of the 22nd International Conference on System Theory, Control and Computing (ICSTCC), Sinaia, Romania, 10–12 October 2018; pp. 691–696. [CrossRef]
37. SPID Protocol. Available online: https://www.agid.gov.it/sites/default/files/repository_files/circolari/spid-regole_tecniche_v1.pdf (accessed on 10 June 2019).
38. Gai, K.; Qiu, M. Blend Arithmetic Operations on Tensor-Based Fully Homomorphic Encryption Over Real Numbers. *IEEE Trans. Ind. Inform.* **2018**, *4*, 3590–3598. [CrossRef]
39. Carretero, J.; Izquierdo-Moreno, G.; Vasile-Cabezas, M.; Garcia-Blas, J. Federated Identity Architecture of the European eID System. *IEEE Access* **2018**, *6*, 75302–75326. [CrossRef]